Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 581-587
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Audit Keamanan Sistem Informasi Pada Data Center Menggunakan Standar SNI-ISO 27001

Syafrinal[1], Agusrijar[2]
STMIK Indonesia Banda Aceh
Frienal@gmail.com[1], Agusrijar83@gmail.com[2]

Abstract

Information system security management is very important for Aceh Government institutions in managing information assets that refer to a standard. This will have a negative impact on the sustainability of information services, especially e-mail services managed by the Aceh Communication, Information and Encryption Service. So the need for good management governance according to national and international standards in order to create good management of electronic mail information system services by conducting an internal audit process on its management in terms of physical and environmental security where the electronic mail service information system is managed. This study discusses the "Information System Security Audit on Data Centers Using SNI-ISO 27001 Standards (Case Study: Aceh Government)". The results showed the need for data and documentation of the final evaluation of the maturity level of the audit process in order to reduce the risk of threats to the information system generated, so that problems can be overcome by making efforts to minimize the possible risks that have been caused. The auditing stages have been carried out on the information system in the data center using the SNI-ISO 27001 standard resulting in a level of maturity still at the "repeatable but intuitive" level that still requires further supervision in the management of the security side.

Keyword: *Security Audit, Indonesian National Standard, Information System*

Abstrak

Manajemen keamanan sistem informasi sangatlah penting bagi institusi Pemerintah Aceh dalam pengelolaan aset informasi yang mengacu pada sebuah standar. Hal ini akan bisa berdampak negatif dari keberlangsungan layanan informasi khususnya layanan surat elektronik (email) yang dikelola oleh Dinas Komunikasi, Informasi dan Persandian Aceh. Sehingga perlunya tata kelola manajemen yang baik sesuai standar nasional maupun internasional agar terciptanya pengelolaan yang baik terhadap layanan sistem informasi surat elektronik dengan melakukan proses audit internal terhadap pengelolaannya dari sisi keamanan fisik dan lingkungan dimana sistem informasi layanan surat elektronik kelola . Penelitian ini membahas tentang "Audit Keamanan Sistem Informasi Pada Data Center Menggunakan Standar SNI-ISO 27001 (Studi Kasus : Pemerintah Aceh)". Hasil penelitian menunjukkan perlunya data dan dokumentasi terhadap evaluasi akhir tingkat kematangan dari proses audit guna mengurangi resiko ancaman terhadap sistem informasi yang ditimbulkan, sehingga permasalahan dapat ditanggulangi dengan melakukan upaya-upaya yang dapat meminimalisir kemungkinan resiko yang telah ditimbulkan. Tahapan-tahapan auditing telah dilakukan pada sistem informasi pada data center dengan menggunakan standar SNI-ISO 27001 menghasilkan tingkat kematangan masih pada level "repeatable but intuitive" yaitu masih memerlukan pengawasan lebih lanjut dalam pengelolaan dari sisi keamanan.

Kata Kunci: *Audit Keamanan, Standar Nasional Indonesia, Sistem Informasi*

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 581-587
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

1. PENDAHULUAN

Dinas Komunikasi, Informatika dan Persandian Aceh (Diskominfo dan Sandi Aceh) yang memiliki wewenang dalam pengelolaan aset teknologi dan informasi pada pemerintah aceh berdasarkan Peraturan Gubernur Aceh Nomor 119 Tahun 2016. Sebagai Institusi yang mengelola Sistem Informasi Pada Pemerintah Aceh, Dinas Komunikasi, Informatika dan Persandian Aceh telah memanfaatkan teknologi informasi dan telah melakukan penerapan layanan-layanan dalam melakukan upaya, agar dapat melakukan tata kelola yang baik terhadap sistem informasi Pemerintah Aceh, hal ini dilakukan agar Pemerintah Aceh dan Pemerintah Kabupaten/Kota di Wilayah Aceh dapat bersinergi membangun layanan handal dan terpercaya dengan membangun infrastruktur bersifat *Local Area Network* dan aplikasi yang sinergi antara pemerintah pusat di Jakarta, pemerintah aceh, dan pemerintah kabupaten/kota dengan melakukan pengelolaan terhadap data center terpusat terutama pada sistem otomasi kantor seperti layanan pengelolaan surat elektronik *(email)* sesuai tugas dan fungsinya mengelola sistem informasi pemerintah aceh.

Proses pertukaran informasi menggunakan layanan *email* memberikan kemudahan dalam menyampaikan informasi tanpa mengenal batas dan waktu , sehingga informasi dalam penyelenggaraan pemerintahan dapat disampaikan dengan cepat dan mudah dalam mendukung proses pembangunan suatu daerah. Jumlah saat ini yang harus dilayanani sebanyak 48 SKPA (Satuan Kerja Perangkat Aceh), rata-rata per satuan kerja nya berjumlah lebih kurang 50 orang karyawan sehingga jumlah keseluruhan pengguna mencapai 2400 orang yang menggunakan layanan email kedinasan. Untuk saat ini layanan bertumpu pada satu perangkat server dengan kapasitas terbatas. Besarnya jumlah pengguna layanan tidak menutup kemungkinan menyebabkan trafik layanan meningkat tinggi, sehingga perlunya pengelolaan sistem infomasi layanan surat elektronik dengan standar yang baik terkait resiko yang ditimbulkan seperti, terganggunya layanan yang disebabkan ketidak stabilan mesin layanan, kepercayaan pengguna terhadap penggunaan surat elektronik yang berdampak pada informasi yang disampaikan tidak utuh diterima oleh pengguna lainnya.
Resiko-resiko yang ditimbulkan menyebabkan aspek keamanan begitu sangat di perhatikan terkait pengelolaan keamanan sistem informasi layanan *e-mail*, sehingga Pemerintah Aceh melalui Dinas Komunikasi, Informatika dan Persandian Aceh menyadari perlunya suatu tata kelola manajemen yang baik sesuai standar, baik nasional maupun internasional, sesuai kebijakan Peraturan Menteri Kominfo Nomor 4 Tahun 2016 Tentang Sistem Manajemen Pengamanan Informasi dengan melakukan audit terhadap keamanan sistem informasi layanan surat elektronik *(e-mail).*

Berdasarkan latar belakang tersebut, penelitian ini mengusulkan untuk melakukan audit keamanan sistem informasi pada Data Center Pemerintah Aceh menggunakan standar SNI-ISO 27001. ISO 27001 merupakan standar internasional yang telah menyediakan kebutuhan untuk membangun,

melaksanakan, menjaga dan terus meningkatkan keamanan informasi dari teknologi informasi untuk sebuah sistem manajemen. Framework yang digunakan adalah SNI-ISO 27001:2013 yang telah memiliki Klausul, Objektive Kontrol, dan Kontrol yang digunakan untuk dijadikan panduan dalam melakukan manajemen terhadap keamanan informasi pada teknologi informasi dari organisasi/lembaga/perusahaan. Untuk penelitian ini menghasilkan dokumentasi hasil audit berupa rekomendasi, evaluasi, temuan untuk perbaikan terhadap kondisi tata kelola data center Pemerintah Aceh yang masih jauh mengacu pada standar manajemen tata kelola yang seharusnya.

2. METODOLOGI PENELITIAN

2.1. Data Center

Menurut Wikipedia (2016) data center merupakan suatu fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen-komponen terkaitnya, seperti sistem telekomunikasi dan penyimpanan data.

2.2. Surat Elektronik

Menurut Kadir. A (2014: p.184) surat elektronik merupakan program yang digunakan untuk menerima atau mengirimkan surat secara elektronik. Alat komunikasi tertulis yang digunakan untuk menyampaikan pesan atau informasi dari pihak yang satu kepada pihak yang lainnnya.

2.3. Audit

Menurut Arens, Alvin A (2015) audit merupakan pengumpulan dan evaluasi terhadap bukti untuk menentukan derajat kesesuaian antara informasi dan kriteria yang telah ditetapkan. Hal ini berarti dalam pelaksanaannya evaluasi dilakukan mengacu pada sejumlah kriteria tertentu untuk menentukan derajat kinerja yang telah dicapai.

2.4. Audit Sistem Informasi

Menurut ISACA, (2016) audit sistem informasi sebagai proses pengumpulan bukti dan pengevaluasian kekuatan dan kelemahan kontrol internal berdasarkan bukti yang dikumpulkan melalui test audit, dan penyiapan laporan dan rekomendasi.

2.5. Keamanan Sistem Informasi

Menurut Komalasari, R dan Perdana, I (2014) keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis, meminimasi resiko bisnis, dan memaksimalkan atau mempercepat pengembalian invenstasi dan peluang bisnis.

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 581-587
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

2.6. SNI-ISO 27001

Menurut Kominfo (2017: p.7) ISO/IEC 27001 berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun sistem manajemen keamanan informasi (SMKI). Standar ini memfokuskan diri pada keamanan sistem informasi suatu organisasi. ISO/IEC 27001:2013 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management System* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi dalam sebuah organisasi/lembaga/perusahaan.

2.7. Maturity Level

Menurut Chaundari. M dan Copra. A (2017: p.11) tingkat kematangan *(maturity level)* adalah jalur yang memastikan organisasi mampu meningkatkan rangkaian area proses berturut-turut secara bertahap. Setiap tingkat kematangan memiliki serangkaian proses yang jika diterapkan bersama, akan membantu anda mencapai satu tingkat kematangan penuh.

Tahapan pelaksanaan Audit mencakup :

a) Perencanaan Audit
b) Persiapan Audit
c) Pelaksanaan Audit
d) Pelaporan Audit

3. HASIL DAN PEMBAHASAN

3.1. Perencanaan Audit

Hasil dari perencanaan audit ini adalah identifikasi proses bisnis, penentuan ruang lingkup, objek, dan tujuan audit, selain itu membuat surat perjanjian, penentuan klausul, objektif kontrol, dan kontrol.

3.2. Persiapan Audit

Hasil dari perencanaan audit ini adalah penyusunan *audit working plan*, daftar penyampaian kebutuhan data, membuat pernyataan, melakukan pembobotan, dan membuat pertanyaan dapat dilihat pada Tabel 1 dan Tabel 2

Tabel 1. Pernyataan dan Bobot

Klausul: A.11 Keamanan Fisik dan Lingkungan		
Objektif Kontrol: A.11.1 Wilayah Aman		
Kontrol A.11.1.1 Pembatasan Keamanan Fisik		
No	Pernyataan	Bobot
1	Adanya pendefinisian parameter keamanan secara jelas (dinding, kartu akses masuk atau penjaga pintu) terhadap ruang pemrosessan	0.6
2	Adanya penggunaan parameter keamanan untuk melindungi ruang fasilitas pemrosessan informasi layanan email	1

Jurnal Sains Komputer & Informatika (J-SAKTI)
Volume 4 Nomor 2, September 2020, pp. 581-587
ISSN: 2548-9771/EISSN: 2549-7200
https://tunasbangsa.ac.id/ejurnal/index.php/jsakti

Tabel 2. Pertanyaan

Klausul: A.11 Keamanan Fisik dan Lingkungan		
Objektif Kontrol: A.11.1 Wilayah Aman		
Kontrol A.11.1.1 Pembatasan Keamanan Fisik		
No	Pernyataan	Pertanyaan
1	Adanya pendefinisian parameter keamanan secara jelas (dinding, kartu akses masuk atau penjaga pintu) terhadap ruang pemrosessan	1. Apakah sudah didefinisikan tentang parameter?
		2. Pendefinisian parameter apa sudah disosialisasikan?
2	Adanya penggunaan parameter keamanan untuk melindungi ruang fasilitas pemrosessan informasi layanan email	1. Sudahkah ada parameter untuk melindungi ruang pemrosessan informasi tersebut?
		2. Parameter apa saja yang terdapat pada gedung/ruang data center?

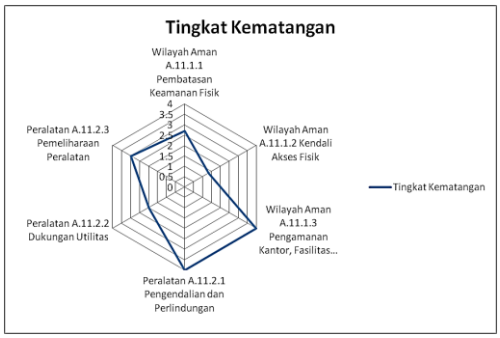
3.3. Pelaksanaan Audit

Pada tahapan pelaksanaan audit ada beberapa langkah dilakukan yaitu melakukan pertemuan pendahuluan audit, wawancara dan observasi, pemeriksaan data dan bukti, melakukan uji kematangan, menyusun temuan dan rekomendasi audit, dan konfirmasi temuan dan rekomendasi. Uji kematangan dapat dilihat pada Tabel 3.

Tabel 3. Uji Kematangan

Klausul: A.11 Keamanan Fisik dan Lingkungan										
Objektif Kontrol: A.11.1 Wilayah Aman										
Kontrol A.11.1.1 Pembatasan Keamanan Fisik										
No	Pernyataan	Hasil Pemeriksaan	Bobot	Penilaian					Nilai
				1	2	3	4	5	
1	Adanya pendefinisian parameter keamanan secara jelas (dinding, kartu akses masuk atau penjaga pintu) terhadap ruang pemrosessan	Pendefinisian dan sosialisasi telah dilakukan Bukti : -Kebijakan Pengendalian keamanan fisik dan lingkungan Gedung Data Center	0.6				✓		2.4
2	Adanya penggunaan parameter keamanan untuk melindungi ruang fasilitas pemrosessan informasi layanan email	Terdapat penggunaan parameter keamanan Bukti : -Foto (finger print, pagar ,dinding, dll) - Penjaga Gedung	1			✓			3
Total Bobot			1.6	TK					2.7

dan contoh hasil representasi keseluruhan tingkat kematangan dalam diagram jaring laba-laba dapat dilihat pada Gambar 1.



Gambar 1. Representasi Tingkat Kematangan

3.4. Pelaporan Audit

Tahapan pelaporan audit adalah memberikan laporan kepada organisasi hasil dari pertanggung jawaban dalam penugasan proses audit. Laporan audit hanya ditujukan kepada kepala seksi keamanan informasi e-government yang memiliki hak saja, dikarenakan dokumen tersebut bersifat rahasia.

4. SIMPULAN

Berdasarkan hasil audit keamanan sistem informasi yang telah dilakukan, maka didapat kesimpulan sebagai berikut :

a) Pelaksanaan evaluasi audit keamanan sistem informasi pada data center telah dilakukan menggunakan standar SNI-ISO 27001:2013.
b) Evaluasi Audit keamanan sistem informasi pada data center menggunakan SNI-ISO 27001:2013 studi kasus Pemerintah Aceh menghasilkan semua dokumen yang dibutuhkan, seperti daftar pernyataan, daftar bobot pernyataan, daftar pertanyaan, dokumen hasil pemeriksaan, perhitungan tingkat kematangan hingga daftar temuan dan rekomendasi yang nantinya akan digunakan sebagai acuan dalam perbaikan-perbaikan terhadap kontrol keamanan sistem informasi.
c) Dari hasil audit keamanan sistem informasi pada data center menggunakan SNI-ISO 27001:2013 studi kasus Pemerintah Aceh didapatkan hasil rata-rata maturity level pada klausul keamanan fisik dan lingkungan yaitu *repeatable but intuitive*. Hal tersebut menunjukan bahwa sebagian besar proses keamanan sistem informasi pada klausul ini sudah terpola dan masih diperlukan koordinasi serta pengawasan lebih lanjut dalam proses bisnis penyelenggaraan dan tata kelola sistem informasi pada layanan.

Beberapa saran yang dapat diberikan untuk proses pengembangan lebih lanjut sebagai berikut:

a) Untuk kedepannya disarankan untuk dilakukan perbaikan terhadap aturan, panduan, prosedur keamanan sistem informasi, kebijakan serta persyaratan yang masih memiliki kekurangan.
b) Dinas diharapkan melakukan audit internal kembali setelah dilakukannya perbaikan-perbaikan terhadap kontrol-kontrol yang masih ada kekekurangan dalam proses pelaksanaannya.

DAFTAR PUSTAKA

[1] Ahmad, A. (2012). *Bakuan Audit Keamanan Informasi Kemenpora.* Indonesia: Kementerian Pemuda dan Olahraga.
[2] Arens, Alvin A. (2015). *Auditing & jasa Assurance*. Jakarta : Erlangga
[3] Chaudhary, M., & Chopra , A. (2016). *CMMI for Development : Implementation Guide*. Penerbit Apress.
[4] Direktorat Keamanan Informasi. (2011). *Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik.* Jakarta: Kementrian Keamanan Informasi dan Informatika RI.

[5] Direktorat Keamanan Informasi. (2017). *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi.* Jakarta: Kementrian Komunikasi dan Informatika RI.

[6] Digdo,G.P (2017). Panduan Audit Keamanan Komputer Bagi Pemula. Jakarta: Elekmedia Komputindo.

[7] IBISA (2013). Physical Security, Mencegah Serangan Terhadap Pendukung Sistem Informasi. Yogyakarta:Andipublisher.

[8] ISO/IEC 27001:2013 (E), (2013). *Information technology – Security techniques – Information security management systems – Requirements*. International Standart.

[9] ISACA, IS Auditing Guidelines-Applications Systems Review-Document (2016). *Information system Auditing: Tools and Techniques-Creating Audit Programs.* USA, Inc. Information Systems Audit and Control Association.

[10] Kadir, A. 2014. Pengenalan sistem informasi Edisi Revisi. Yogyakarta: Penerbit Andi.

[11] Komalasari, R., & Perdana, I. (2014).Audit Keamanan Informasi Bagian Teknologi Informasi PT. PLN (Persero) DJBB Menggunakan SNI ISO/IEC 2007:2009. *Jurnal Sistem Informasi, IX* (2) 201 – 216.

[12] Krismiaji, 2015. Sistem Informasi Akuntansi, Penerbit: Yogyakarta.

[13] Mahdianta Pandia, 2013. Penerapan Keamanan Sistem Informasi Standar ISO 27001 Pada PT. BPR KARYA BHAKTI UGAHARI TANJONG MORAWA. Medan: Jurnal Ilmiah Ekonomi, Hukum, Pertanian, Peternakan, Kedokteran, Pendidikan, Komputer. Vol.4, No.1 .68-73.

[14] Winarno, W.W. (2017). Sistem Informasi Manajemen.(Edisi ke-3).STIM YKPN.

[15] Wikipedia bahasa indonesia. *"Pusat Data",* 27 Agustus 2018 https://id.wikipedia.org/wiki/Pusat_data.

[16] Yulindra.(2014). *Keamanan Sistem Informasi*: STMIK ATMA LUHUR. Yogyakarta:Deepublish